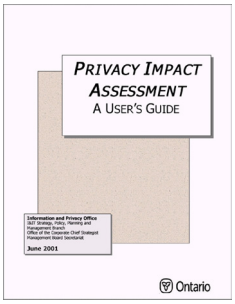
PIA
プライバシー影響アセスメントとは何か？



カナダ・オンタリオ州政府発行のPIAガイドブック（「参考資料」参照）

カナダの事例にもとづく考え方の紹介

2005.7.19

Ver.1.0

移住連学習会

於：弁護士会館

西邑 亨

office dlc

PIA / PET などの日本国内での紹介について

- PIA（プライバシー影響アセスメント）やPET（プライバシー強化技術）など、ネットワーク社会における個人の「プライバシー」確保のための技術や知識・手法などの紹介は、国内では、以前からメタア・ソシエイツのタカマ・ゴースケさんがほとんどひとりで努力してこられました。彼の努力の成果もあり、技術的知見としてのPIAやPETは、以前からICT技術者の間では少しずつ知られており、断片的な利用はさまざまな形で行われてきたようです。しかし、これらを総合的に導入したシステム構築が行われたという報告は、現在のところ国内では見あたりません。
- 3年ほど前から、CPSR/Japan（社会的責任を考えるコンピュータ専門家の会日本支部）が、グループの主要な取り組みテーマとしています。同会の伊藤穣一さん（ネオテニー代表）などが政府の調査研究資金を獲得して調査研究を2年間にわたって行うなど（2年目は総務省内の研究会）、CPSR/Japanのメンバーを中心とした組織的な紹介が継続して行われています。
- CPSR/Japanの紹介活動は、日本政府のIT担当者などをターゲットにしたもので、インターネット上で積極的に資料公開されているとはいえ、一般の市民にはほとんど知られていません。
- 市民団体の中では、JCA-NETや情報公開クリアリングハウスなどが強い関心を向け、自治体職員や地域住民、市民団体向けの紹介を試みようとしてきましたが、具体的な活動には直結していません（2グループの共同プロジェクトは、人的資金的問題のためながらく中断状態になっています）。
- また、東京・国分寺市議会は、参考人意見聴取（2004.2.6）の中でPETを取り上げ、市長はじめ多数の市職員らも積極的に傍聴して強い関心を示していました。

（2005.7.19）

PIA
プライバシー影響アセスメント
とは何か?

もくじ

PIA / PET などの日本国内での紹介について

PIAの概要
- PIAの目的
- PIAを構成する3つの要素
- PIAと「個人情報保護」の関係
- PIAは何を対象とするのか
- PIAは誰が実施するのか
- PIAが前提とする環境要件
- PIAの手順
- プライバシー要件の特定
- PIAの実施
- PIAにおける処理フロー収集の例
- PIAが採用するプライバシー測定の客観的基準
- プライバシーアーキテクチャーの役割
- PETの例

PIAの課題(日本的な課題)
- 結果は「ガイドライン」に依存する
- プライバシー概念が錯綜している
- 実効性は実施環境に依存する

PIAの導入
- PIA導入に向けた(日本の)課題
- PIA有効活用のための要件

参考資料

PIAの概要

PIAは、「思想」や「規則」ではない

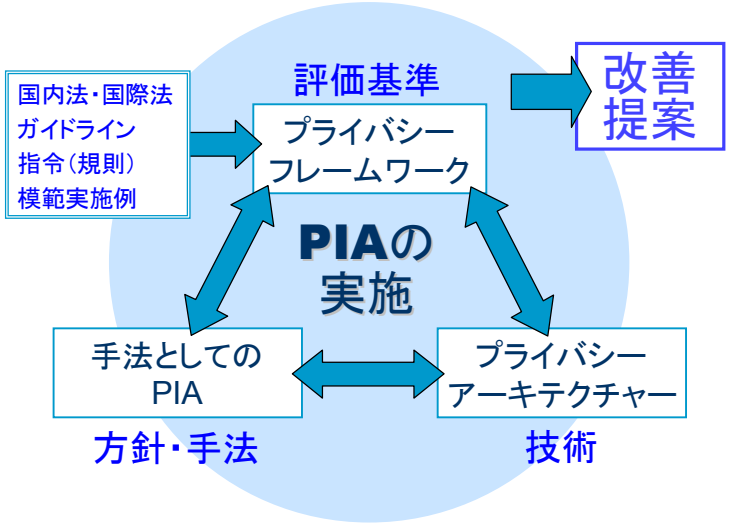
PIAは、「手法」である

主要な参考資料
Peter Hope-Tindall "PRIVACY IMPACT ASSESSMENT FOR E-GOVERNMENT"
＊総務省研究会報告書「参考資料II」(スライド末尾の「参考資料」参照)
ただし、このスライドの作成者(西邑)はかならずしも本資料の筆者と同じ考え方をしているわけではなく
このスライドは、資料の忠実な内容紹介を意図するものではない

PIAの目的

- 個人情報を運用するシステムに対して、個人情報提供者（データ主体）の「プライバシー」に与える「脅威」（リスク）を測定・分析・評価し、その結果から
  - 「プライバシー」リスクの低減に有効な情報を見いだす
  - この情報にもとづいた、事業・施策の策定、システム設計・調達などに必要な具体的提案（改善案）を提出する
  - 個人情報運用システムの透明性を確保し、システム運用者とデータ主体の間の信頼関係形成を支援する

PIAを構成する3つの要素



PIAと「個人情報保護」の関係

- PIA（プライバシー影響アセスメント）
  - 個人（システムに個人情報を提供するデータ主体）の利益のために行われる活動

目的はまったく別のもの　利害対立もありうる

- 個人情報保護（運用者の利益：手段としての本人の損害回避）
  - システム運用者が、データ主体にリスクがおよぶ個人情報の運用について、運用者の社会的正当性を確保するために行う活動

PIAは何を対象とするのか

- 個人情報を運用する「システム」の全体
  - システムに関わるネットワークの全体
  - システムに関わるコンピューターとソフトウェア全体
    - 関連する人的な組織・業務手順・各種関連規則のどこまでを対象とするかについては、実施者の任務や権限によると思われる
- PIAが準拠する法制度等（ガイドライン等）は原則として対象外
  - 「プライバシー・フレームワーク」（個別作業のための判断基準：プライバシー要件）を明確化することは、PIA作業の範囲
    - 従って、「プライバシー」に関わる法制度が未整備な状態にある日本では、「プライバシー・フレームワーク」の整備作業は、むしろPIAの主要な業務であり得る
- PIAが実施されるタイミング：
  新システムの企画・設計／従来システムの改修・機能追加などの時点

PIAは誰が実施するのか

- システム設計および業務担当セクション
  - 上位の「プライバシー」政策セクションに報告(USA)
  - 最終的にプライバシー監督局に報告（カナダ）
    - PIAが完了しなければ、予算は執行されない（カナダ・USA）

- データ主体を含む利害関係者（stakeholders）
  - 「韓国ではマルチステークホルダー＊によるテクノロジーインパクトアセスメントを実施している と聞いたことがある。」（Openlaw＊＊にあったコメント）

＊：複数の利害関係者。最近の国連の会議では、国境を越える課題について、各国政府だけでなく利害を持つ市民社会（Civil Society）や企業部門（Privete Sector）などが対等の立場で意思決定参加することが定着してきている。この方式を国内課題についても適用しようとしているように見える（日本の「市民参加」とはかなり意味が違う）。

＊＊：Openlaw：電子政府・電子自治体の情報セキュリティ問題をテーマとしてCPSR/Japan　のプロジェクトが運営するブログサイト（http://openlaw.g.hatena.ne.jp/s-yamane/）

PIAが前提とする環境要件

- プライバシー・ガイドライン（必要ならPIA作業で検討）
  - 明確な「プライバシー」の定義
  - プライバシー状況の具体的評価基準としての「規則」
- プライバシー強化技術（PET）
  - プライバシー保障のための体系的技術手段
- 実用的なレベルの情報セキュリティ強度

- システム運用者側の透明性と説明責任
  - システム運用者とデータ主体間の信頼関係
- PIA実施の制度的位置づけと社会的意欲

PIAの手順

① 実施計画の作成
- 適切なメンバー構成と任務
- 作業手順とスケジュール

② プライバシー要件の特定（ガイドラインの整理）
- 対象の特性に合わせた判断基準の収集・整理（プライバシーフレームワークの構築）

③ PIAの実施
- 対象の分析・評価の実施
- 改善のための、設計・技術導入・運用などの提案

プライバシー要件の特定

（対象に適合するプライバシーフレームワークの構築）

- 対象業務に適用される制度的義務を網羅的に列挙する
  - 国内法・国際法
  - ガイドライン（各種規則）
  - 指令（行政的な指示として出された規則など）
  - 模範実施例
- 対象業務に特性に応じて、重点的に配慮すべきプライバシー要件が存在する場合がある

PIAの実施

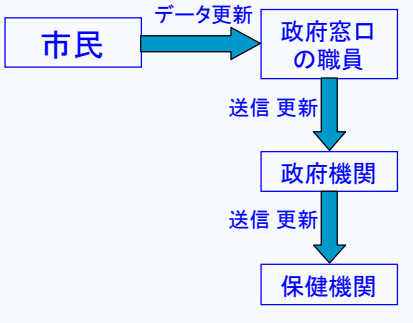
① 個人情報とその処理フローのリストアップ
- システム設計書などから網羅的に収集

② プライバシー測定
- 処理フローごとに客観的基準によって判定する
  - 個人特定性・結合性・観察容易性（PIA独自の客観的評価基準）

③ 分析・評価（事前分析）
- プライバシーフレームワークに基づいて、処理フロー及び全体に関するプライバシー侵害の脅威と防御対策について総合的に分析・評価する

④ フォローアップ分析
- 設計、構築、改修などのステップごとに、上記①、②、③を実施する、など

PIAにおける処理フロー収集の例



データ項目
市民ID
健康保険番号
医師ID／氏名
患者氏名
生年月日
住所
性別
日付
同意有無

西邑注：この例は、個人情報の「流通モデル」になっており、改善の余地があると考えられる

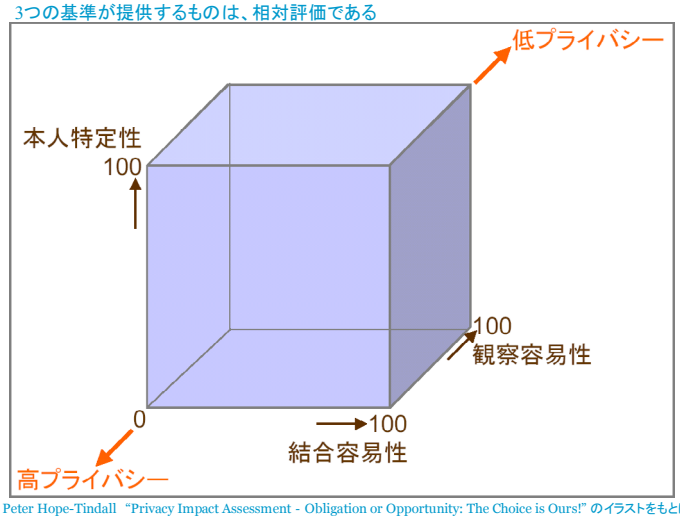
仮想された健康に関する行政サービス窓口業務の一例
Peter Hope-Tindall "Privacy Impact Assessment - Obligation or Opportunity: The Choice is Ours!" のイラストより作成

PIAが採用する プライバシー測定の客観的基準

- 個人特定性(Identity)あるいは匿名度(nymity)
  - 当該の情報によって個人を特定できる程度を測定する基準。「完全に匿名(個人名がまったく特定されない状態)」から「完全に実名(本名が特定された状態)」という範囲で測定される。
- データの結合性(Linkability)
  - 複数のオペレーションで得られたデータを付き合わせて個人を特定するような行為からユーザーがどの程度守られているか
- システムにおける観察容易性(Observability)
  - あるシステムが使用されたことにより、個人特定性やデータ結合性がどの程度影響を受けるか
- どんな場合でも、PIAが目標とするのは、「個人の特定性」、「データの結合性」、そして「システムにおける観察容易性」の3 要素を最小限に抑えること

PIAが採用する プライバシー測定の客観的基準

3つの基準が提供するものは、相対評価である



Peter Hope-Tindall "Privacy Impact Assessment - Obligation or Opportunity: The Choice is Ours!" のイラストをもとに西邑作成

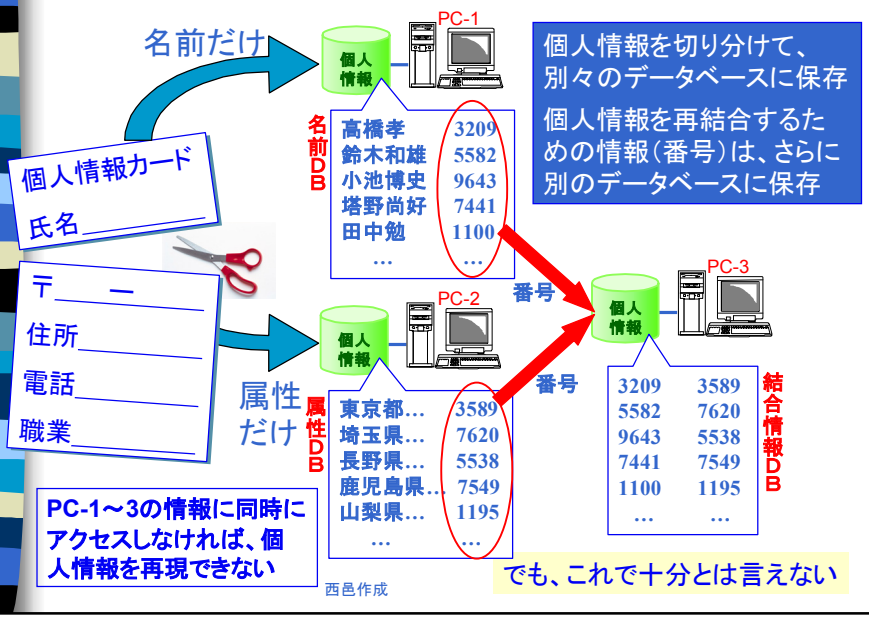
プライバシーアーキテクチャーの役割

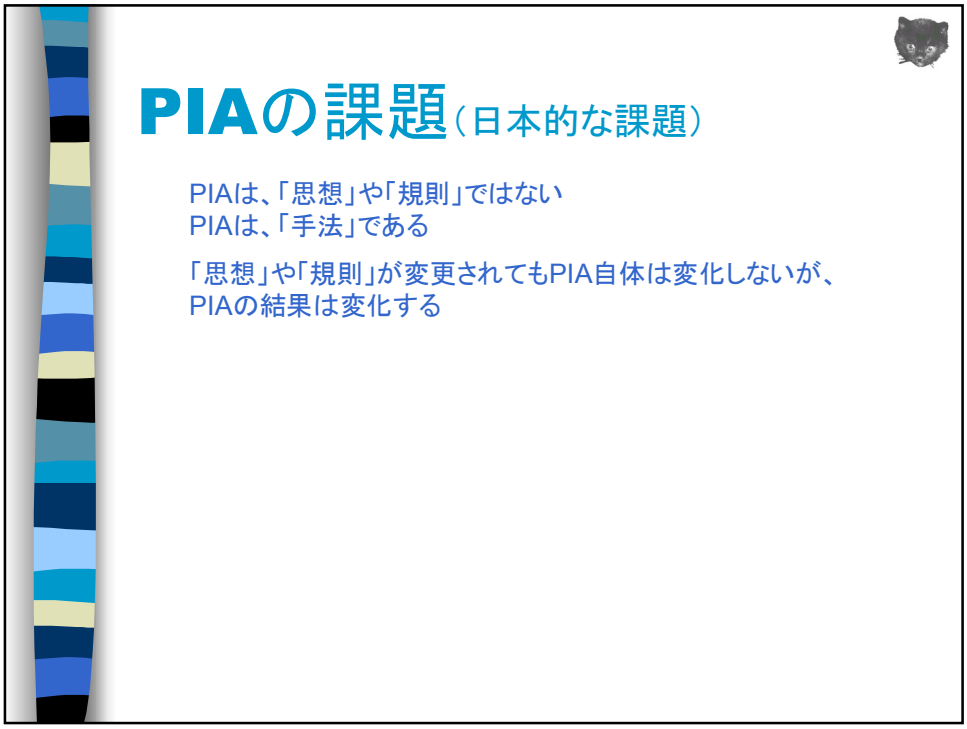
- 実際に「設計にプライバシー対策を組み込む」ことを可能にする仕組みである。これは(PIA 同様)プライバシー・フレームワークを補完するが、プライバシー・アーキテクチャーが関わるのは、ポリシーの変化ではなくアーキテクチャーの改良であり、運営管理面ではなく技術管理面であり、法律や指令ではなくハードウェア面である。

Peter Hope-Tindall "Privacy Impact Assessment - Obligation or Opportunity: The Choice is Ours!"

「プライバシーアーキテクチャー」は、プライバシー強化技術(PET)を実装するための技術的な手法を提供するもの

PETの例

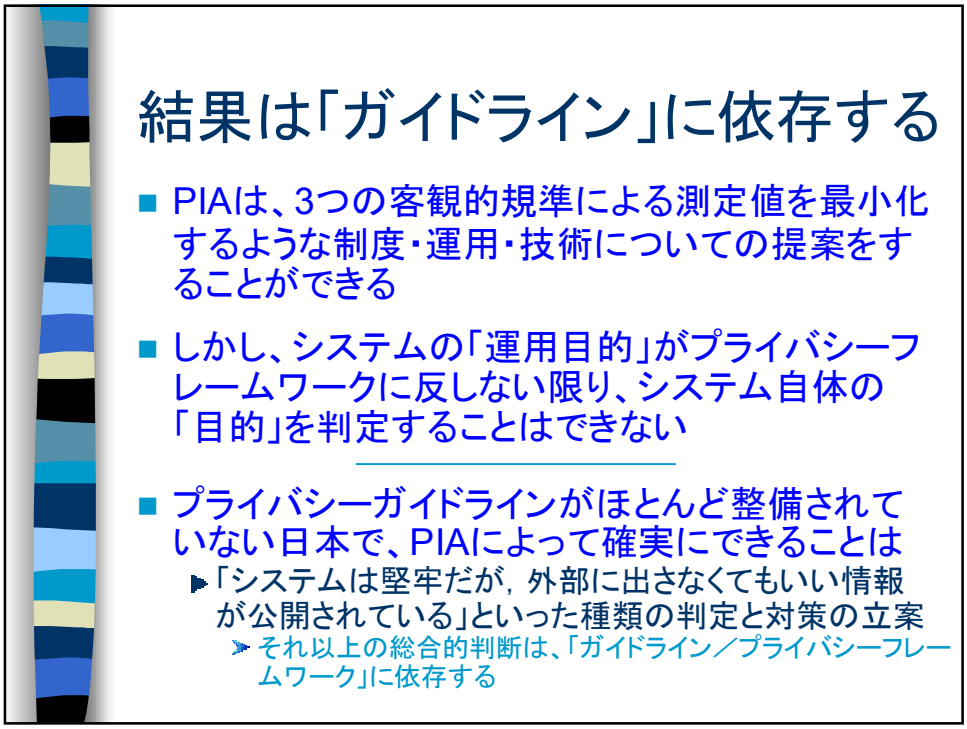




PIAの課題（日本的な課題）

PIAは、「思想」や「規則」ではない
PIAは、「手法」である

「思想」や「規則」が変更されてもPIA自体は変化しないが、
PIAの結果は変化する



結果は「ガイドライン」に依存する

- PIAは、3つの客観的規準による測定値を最小化するような制度・運用・技術についての提案をすることができる
- しかし、システムの「運用目的」がプライバシーフレームワークに反しない限り、システム自体の「目的」を判定することはできない
- プライバシーガイドラインがほとんど整備されていない日本で、PIAによって確実にできることは
  - 「システムは堅牢だが，外部に出さなくてもいい情報が公開されている」といった種類の判定と対策の立案
    - それ以上の総合的判断は、「ガイドライン／プライバシーフレームワーク」に依存する

プライバシー概念が錯綜している

- 「ネットワーク社会」における「私的領域への干渉の脅威（プライバシーの危機）」に対する無理解
- 「個人情報＝プライバシー」という錯綜
  - 「自己情報コントロール権」の錯綜
  - リアル社会とネットワーク社会の錯綜
- 「自己決定によりプライバシーが放棄されている」とする行政が持つ個人情報の神話
  - 行政内部における「情報結合」のフリーハンド
- 「プライバシーより公共の福祉が（無前提的に）優先する」という俗説
  - たとえば「治安維持」という聖域

プライバシー概念が錯綜している

- 民間の関係における個人の「プライバシー」

この2つは、本来異なる性格を持つが
それが社会的に理解されていないように見える

- 行政との関係における個人の「プライバシー」

- 行政には、「情報結合」から得られる利益を、民間と同じように獲得することが許されるか？（社会的合意の不在）

まず住基ネットによって多くの人が心配しているのは、それによって「自己の情報を関連づけられるということ(linkability)」ではないかと思わ れる。日本国内において「自己の情報を関連づけられない(unlinkability)」権利がどの程度認められるか否かは最終的には司法の判断によると ころだ。

＊武田圭史「住基ネットは情報セキュリティの問題ではない」2005.6.5
http://motivate.jp/archives/2005/06/post_58.html

実効性は実施環境に依存する

- 実際、カナダでは、政府及び地方の関係省庁が予算を承認する場合、新たな技術、プログラム、評価対象の計画に関する実作業の開始前に、何らかの形でPIA を提出することが義務付けられている。しかし残念なことに、これはPIA に対する「義務としてやらざるをえないもの」という見方をさらにあおることになり、ただでさえ厄介なプロジェクト申請や予算獲得のプロセスに、新たなハードルを 1 つ増やしただけに留まっている。

Peter Hope-Tindall "Privacy Impact Assessment - Obligation or Opportunity: The Choice is Ours!"

システム運用者側の透明性と説明責任、PIA実施の制度的位置づけと社会的意欲（プライバシー保障への関心と意欲）がきわめて低い日本的状況の中で、PIAが「環境アセスメント」と同様、新規「公共事業」推進の単なる手続きにされる可能性はきわめて高い

PIAの導入

「思想」や「規則」が変更されてもPIA自体は変化しないが、
PIAの結果は変化する
だから、「思想」や「規則」は別の手続きによって
社会的に合意されている必要がある

だが、私たち自身のプライバシー確保のために
私たちはどのように「社会的合意」を形成することができるのか？

PIA導入に向けた（日本の）課題

- 「プライバシー」の定義・ガイドラインの整備
  - 「個人情報保護」との明確な区分
  - 「人権原理」の意識的導入
    - 「自己情報コントロール権」の限界を超える判断基準
  - 「ネットワーク社会」の正確な理解
    - 「ネットワーク社会」は “Surveillance Society” ＊でもある
- 実施者（監督者）の任務と権限
  - データ主体利益の確保（任務の明確化）
  - 実効性の担保（調査・命令・予算承認権など）
- 透明性の確保
  - 公正性・正確性の担保

＊: David Lyon “Surveillance Society” 2001／『監視社会』 河村一郎訳　青土社

PIA有効活用のための要件

- 「本人の利益」という目的の維持確保
  - 複数の「利害関係者」が共同で実施するなど
- 政策立案の初期からの適用
  - 政策的意思決定過程への「参加」の手法としての採用など
    - 資金投入や制度変更がされる前（制約条件が大きくなる前）に、PIAによる改善が実施できることなど
- 適用範囲を限定しない
  - 「プライバシー」の範囲を広く解釈する
  - 「対象システム」の範囲を限定しない

参考資料

以下には、PIAだけでなくPET（プライバシー強化技術）やプライバシー監督局（第三者機関）についての情報が含まれる

- 国際的なガイドライン（明治大学夏井研究室サイトより）

  http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/index.htm

  OECD 8原則（1980）
  OECD プライバシー保護と個人データの国際流通についてのガイドライ

  国連ガイドライン（1990）
  国際連合 コンピュータ化された個人データ・ファイルに関するガイドライン

  UE指令（1995）
  個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令

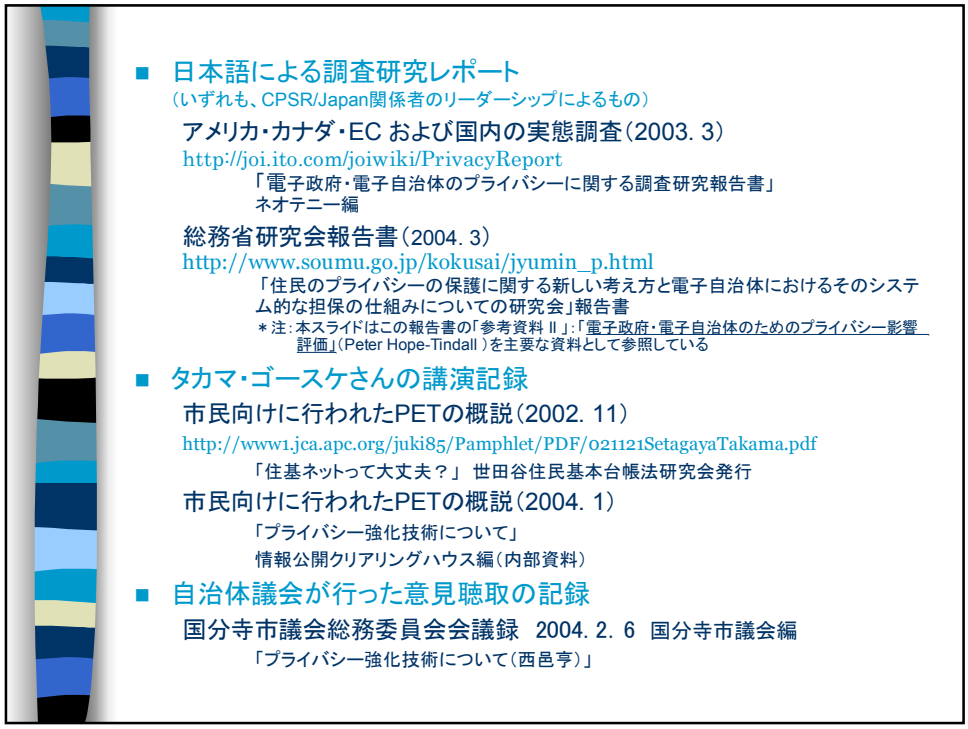
- 英文の報告（カナダ州政府）

  オンタリオ州政府 PIAガイドブック（June 2001）

  http://home.inter.net/gt/grabbag/Ontario_pia1.pdf
  “PRIVACY IMPACT ASSESSMENT A USER'S GUIDE”
  Information and Privacy Office (Ontario)

  アルバータ州政府 プライバシーアーキテクチャー概説（May 2003）

  http://home.inter.net/gt/grabbag/AlbertaPrivacyArchitecture.pdf
  “PRIVACY ARCHITECTURE OVERVIEW””
  Government of Alberta



- 日本語による調査研究レポート
  （いずれも、CPSR/Japan関係者のリーダーシップによるもの）
  - アメリカ・カナダ・EC および国内の実態調査（2003. 3）
    http://joi.ito.com/joiwiki/PrivacyReport
    「電子政府・電子自治体のプライバシーに関する調査研究報告書」
    ネオテニー編
  - 総務省研究会報告書（2004. 3）
    http://www.soumu.go.jp/kokusai/jyumin_p.html
    「住民のプライバシーの保護に関する新しい考え方と電子自治体におけるそのシステム的な担保の仕組みについての研究会」報告書
    ＊注：本スライドはこの報告書の「参考資料Ⅱ」：「電子政府・電子自治体のためのプライバシー影響評価」（Peter Hope-Tindall ）を主要な資料として参照している
- タカマ・ゴースケさんの講演記録
  - 市民向けに行われたPETの概説（2002. 11）
    http://www1.jca.apc.org/juki85/Pamphlet/PDF/021121SetagayaTakama.pdf
    「住基ネットって大丈夫？」 世田谷住民基本台帳法研究会発行
  - 市民向けに行われたPETの概説（2004. 1）
    「プライバシー強化技術について」
    情報公開クリアリングハウス編（内部資料）
- 自治体議会が行った意見聴取の記録
  - 国分寺市議会総務委員会会議録　2004. 2. 6　国分寺市議会編
    「プライバシー強化技術について（西邑亨）」